3 システムのセットアップ

購入後、初めて本製品をセットアップする時の手順を説明します。二重化構成を構築する場合は、4章を参照してください。

セットアップの概要

セットアップには、本体以外のマシンや接続のためのケーブルなどが必要となります。また、それぞれのマシンについてもソフトウェアのインストールなどの準備が必要となります。

- **本体**

  購入時のハードディスク上にはFireWall-1(Linux版)のモジュール、および基本設定ツールがインストール済みです。こちらを使用して、コンフィグレーションをしてください。

- **管理クライアント**

  システムの基本設定をするために使用する管理コンピュータとして使用します。
  また、ポリシー作成用のクライアントPC(Windows 98/NT/2000/XPで動作するネットワーク上のコンピュータ)には、本装置に同梱されている「Check Point Next Generation(Feature Pack3)」のCD-ROMからモジュールやGUIクライアントをインストールしてください。初期導入設定用ディスクの作成用としても使用します。
  詳しくはこの後の説明を参照してください。

セットアップには、以下の3通りの方法があります。

- セキュアシェル(SSH)を使用したセットアップ
- Web Management Console(WbMC)を使用したセットアップ
- コンソールを使用したセットアップ

本書では、以降セットアップについて「SSHを使用したセットアップ」を例にとって記述します。
ただし、SSHのクライアントソフトはお客様でご用意ください。

セットアップ

システムをセットアップする方法の中で、セキュアシェル(SSH)を使用した手順を説明します。

設定手順の流れ

設定手順の流れを以下に示します。

1. 初期導入設定用ディスクによる設定

1. 初期導入設定用ディスクの作成
2. 初期導入設定用ディスクによるセットアップ

2. システムのセットアップ

1. 基本設定ツールによる設定
2. FireWall-1のコンフィグレーション

3. セキュリティポリシーのセットアップ

4. バックアップ

5. ESMPRO/ServerAgentのセットアップ

6. システム情報のバックアップ

7. 管理コンピュータのセットアップ

1.　初期導入設定用ディスクによる設定

初期導入設定用ディスクでの設定方法について説明します。

初期導入設定用ディスクの作成

「初期導入設定用ディスク」はFirewallを設定するために最低限必要となる設定情報を保存したセットアップ用のフロッピーディスクです。
添付の「初期導入設定用ディスク」にあらかじめ入っている「初期導入設定ツール」を使用して作成します。「初期導入設定ツール」は、Windows 98/Me/NT4.0/2000/XPが動作するコンピュータで動作します。

初期導入設定ツールの実行と操作の流れ

次の順序で初期導入設定用ディスクを作成します。それぞれの設定項目については、この後に説明しています。

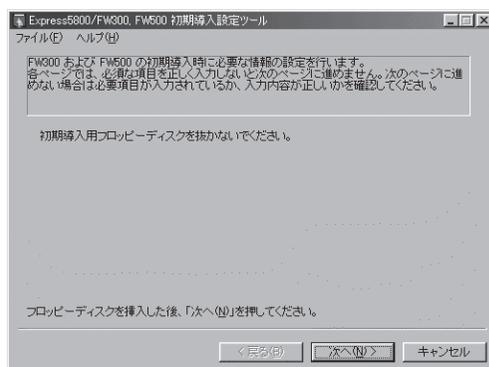
1. Windowsマシンのフロッピーディスクドライブに添付の「初期導入設定用ディスク」をセットする。

2. フロッピーディスクドライブ内の「初期導入設定ツール(StartupConf.exe)」を実行する。

   「初期導入設定ツール」が起動します。

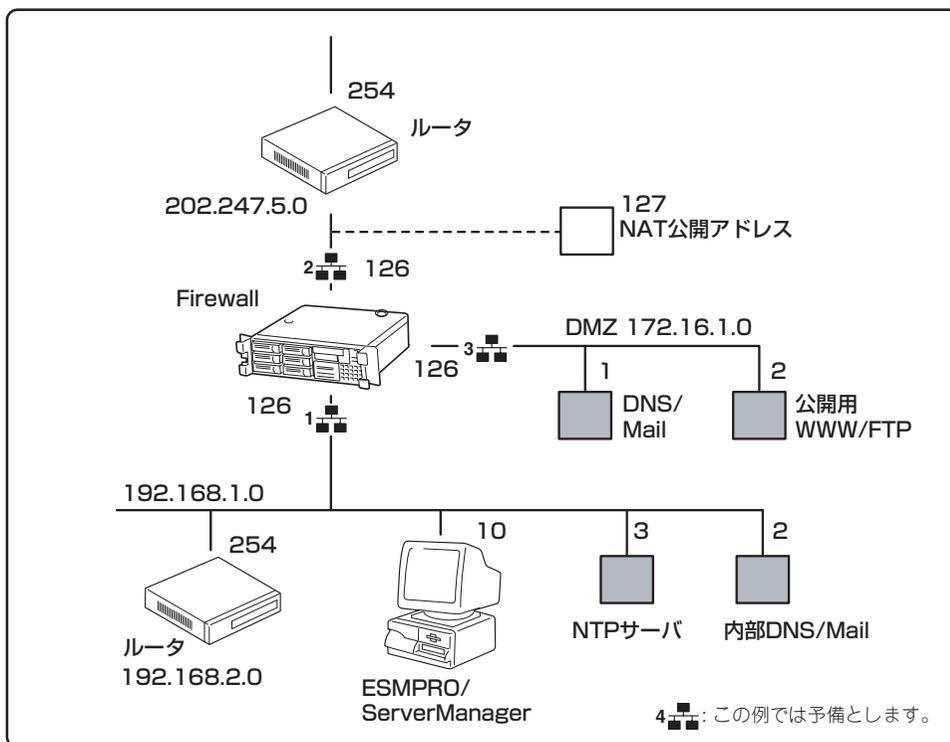
3. 開始画面が表示されたら[次へ]をクリックし、設定の入力を開始する。

   プログラムは、ウィザード形式となっており、各ページで設定に必要事項を入力して進んでいきます。
   必須情報が入力されていない場合や入力情報に誤りがある場合は警告メッセージが表示されますので、項目を正しく入力し直してください。入力事項の詳細については、後述の説明を参照してください。
   すべての項目の入力が完了すると、フロッピーディスクに設定情報を書き込んで終了します。

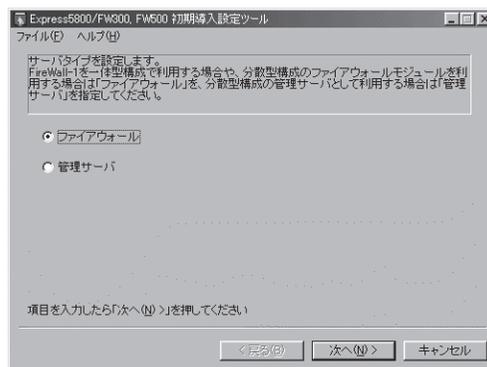
4. 初期導入設定用ディスクをフロッピーディスクドライブから取り出し、「初期導入設定用ディスクによるセットアップ」に進む。

重要

初期導入設定用ディスクは再セットアップの際にも使用します。大切に保管してください。

入力項目の設定

以下のネットワーク構成を例にして「初期導入設定ツール」で入力する項目について説明します。

● **サーバタイプ(設定必須)**

Firewallの種別について設定をします。

システムのセットアップ

● **ネットワークインタフェースの設定**

Firewallのネットワークの設定をします。

- ホスト名(設定必須)

  ホスト名はドメイン名まで含めたFQDNの形式で入力してください。

- LANポート1(設定必須)

  IPアドレス

  LANポート1に割り当てるIPアドレスを入力します。

  サブネットマスク

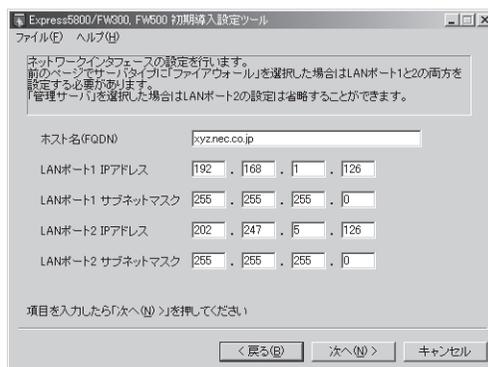
  LANポート1に割り当てたIPアドレスに対するサブネットマスクを入力します。

- LANポート2

  IPアドレス

  LANポート2に割り当てるIPアドレスを入力します。

  サブネットマスク

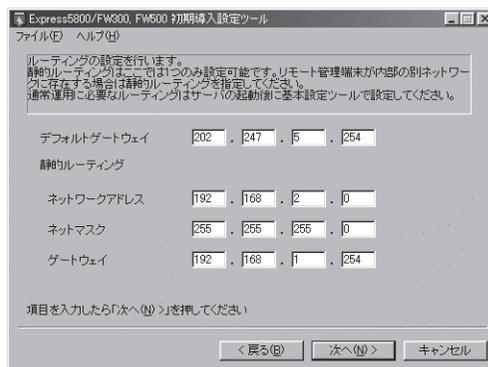
  LANポート2に割り当てたIPアドレスに対するサブネットマスクを入力します。

● **ルーティングの設定**

ネットワークのルーティングの設定をします。

- デフォルトゲートウェイ(設定必須)

  デフォルトゲートウェイのIPアドレスを指定します。

- 静的ルーティング

  宛先ネットワークアドレスとネットマスクおよびゲートウェイの組み合わせを指定します。

● **メールアドレスの設定**

メールアドレスとリモートメンテナンス機能の利用に関する設定をします。

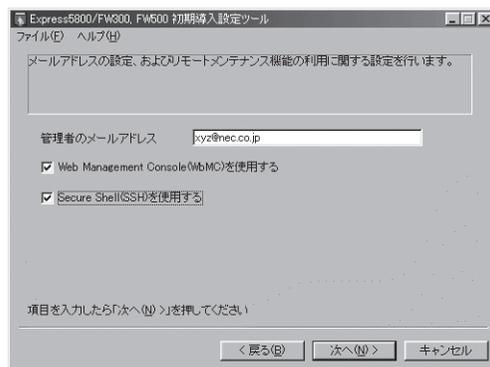
― 管理者のメールアドレス(設定必須)

　管理者のメールアドレスを指定します。

― Web Management Console(WbMC)の設定

　WbMCを使用する場合に、チェックをつけます。

― セキュアシェル(SSH)の設定

　SSHを使用する場合に、チェックをつけます。

● **WbMCに関する設定**

WbMCに関する設定をします。

― WbMCポート番号

　使用するポート番号を入力します。既定値は、18000です。必要に応じて変更してください。

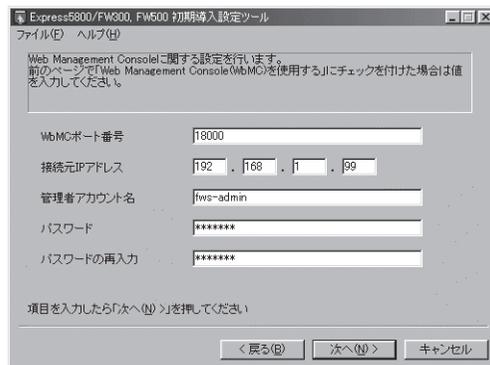
― 接続元IPアドレス

　接続元の管理クライアントのIPアドレスを入力します。

― 管理者アカウント名

　上記で設定した接続元IPアドレスの管理クライアントからWbMCに接続する際の管理者名(15文字以内)を入力します。

― パスワード

　上記で設定した管理者名に対する、パスワードを設定します。

- **SSHに関する設定**

  SSHに関する設定をします。

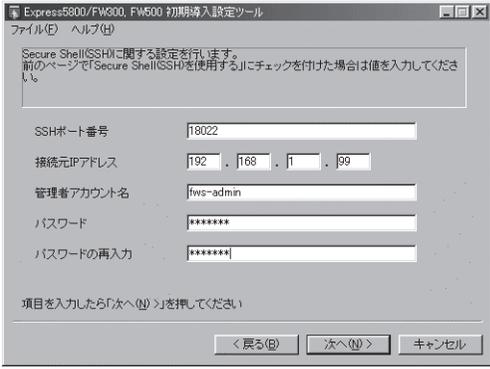
  - SSHポート番号

    使用するポート番号を入力します。既定値は、18022です。必要に応じて変更してください。

  - 接続元IPアドレス

    接続元の管理クライアントのIPアドレスを入力します。

  - 管理者アカウント名

    上記で設定した接続元IPアドレスの管理クライアントからSSHで接続する管理者名(15文字以内)を入力します。

  - パスワード

    上記で設定した管理者名に対する、パスワードを設定します。

初期導入設定用ディスクによるセットアップ

初期導入設定ツールで作成した「初期導入設定用ディスク」を使用して、セットアップし、管理クライアントを本体へ接続します。

セットアップ手順

以下の手順でセットアップします。
正しくセットアップできないときは、次ページを参照してください。

1. SSH通信用ソフトウェアがインストールされている管理クライアントを用意する。
2. 本体の電源がOFFの状態で、管理クライアントと本体背面にあるLANポートインタフェース(内部ネットワーク用)をクロスケーブルで接続するか、本体が接続されている内部ネットワークのハブなどに管理クライアントのLANケーブルを接続する。本体背面のポート番号の表記とLANポートの番号(1、2)は逆になります。本体に1と表記されているポートがLANポート2、2と表記されてるポートがLANポート1となります。また、N8100-104のネットワークインタフェースを増設している場合は、N8100-104のポートがLANポート1、本体に2と表記されているポートがLANポート2になります。
3. 前述の「初期導入設定用ディスクの作成」で作成した初期導入設定用ディスクを本体のフロッピーディスクドライブにセットする。
4. 本体のPOWERスイッチを押す。

   POWERランプが点灯します。しばらくすると、初期導入設定用ディスクから設定情報を読み取り、自動的にセットアップを進めます。2〜3分ほどでセットアップが完了します。
5. 管理者クライアントから初期導入設定用ディスクで設定したSSHに関する設定の「管理者アカウント名」と「Password」を使用し、ログインする。

6. ログイン後、rootユーザーに変更する。

Passwordには、同梱の「rootパスワード」に書かれているパスワードを入力します。

これで初期導入設定用ディスクによるセットアップ、管理クライアントの接続は完了です。
以降の説明では、管理クライアントからの操作でシステムのセットアップを行います。

セットアップの完了が確認できたらセットした初期導入設定用ディスクをフロッピーディスクドライブから取り出して大切に保管してください。再セットアップの時に使用することができます。

セットアップに失敗した場合

システムのセットアップに失敗した場合は、自動的に電源がOFF（POWERランプ消灯）になり、ユーザーに異常終了したことを知らせます。正常にセットアップを完了できなかった場合は、初期導入設定用ディスクに書き出されるログファイル「logging.txt」の内容を確認し、再度初期導入設定ツールを使用して初期導入設定用ディスクを作成してください。

〈主なログの出力例〉

- 「Error: cannot open: /mnt/floppy/fwsinit.ini」

  → 初期導入設定用ディスク中の設定に誤りがある場合に表示されます。

- 「Error: bad user name (WbMC)」

  → 初期導入設定用ディスク中のWbMCの管理者名の指定に誤りがある場合に表示されます。

- 「Error: bad user name (SSH)」

  → 初期導入設定用ディスク中のSSHの管理者名の指定に誤りがある場合に表示されます。

- 「Error: fwsetup failure.」

  → Firewallへ初期導入設定ができない場合に表示されます。初期導入設定用ディスクの設定に誤りがあります。

初期導入設定用ディスクの内容が誤っていた場合、初期導入設定用ディスクの設定内容を修正して再度本体をセットアップすることができます。
以下の操作を行った場合には、初期導入設定用ディスクによる設定の機能はOFFになります。基本設定ツール(fwsetup)もしくはWbMCからのみ設定変更が可能となりますので注意してください。

- 基本設定ツール(fwsetup)を実行し、「replace startup-scripts?」の問に対して〈y〉を入力した場合。
- WbMCの基本設定画面から[設定]を押した場合。

2. システムのセットアップ

「1. 初期導入設定用ディスクによる設定」で管理クライアントからFirewall本体に接続するための最低限必要なセットアップが完了しました。ここからは、ネットワークインタフェースの設定(nicsetup)と基本設定ツール(fwsetup)を使用して、さらに詳細なセットアップを行います。

Firewall本体のホスト名、IPアドレス、ルーティングなどの初期導入設定用ディスクで設定した項目(下記の設定内容の項目における★印の項目)については、設定値を確認してください。

fwsetupのセットアップを実行し、再起動したら、次にcpconfigコマンド使ってコンフィグレーションを行います。

ネットワークインタフェースとCPU増設の設定

ネットワークインタフェースやCPUの増設を行った場合は、基本設定ツールによる設定の前に以下の作業を行います。

- **ネットワークインタフェース(NIC)の増設を行った場合**

  /opt/necfws/bin/nicsetupコマンドを実行して、増設したPCIスロットの位置とネットワークインタフェースの型番を対応付けます。
  また、コマンドの最後でLANボードのレイアウトが簡易表示されます。

```
# /opt/necfws/bin/nicsetup

Please select inserted NIC for each PCI slot.

No. N-Code     NIC Info
 0. ---------  not used
 1. N8104-84   1000BASE-SX board
 2. N8104-86   100BASE-TX board (2 ports)
PCI slot [1B] select No.(0-2)[0]:
   :
 〈省略〉
   :
[LAN port layout (backplane image)]
According to your selection, network interface names
are allocated for NICs as follows after reboot.

  3C:----                       3B:eth3/eth4
  2C:----   OnBoard2:eth1   2B:----
  1C:eth0   OnBoard1:eth2   1B:----
```

増設したNICの番号を選択。増設していない場合は、0を入力する。

装置背面のLANポートのレイアウトが簡易表示される。

PCIスロットの番号

- **CPUの増設を行った場合**

  /boot/grub/grub.confファイルの以下の行を修正します。

  [修正前] default=1

  [修正後] default=0

基本設定ツールによる設定

基本設定ツールの項目や実際の手順の流れを示します。

設定内容

基本設定ツールでの設定項目およびそれぞれの制限事項は以下のとおりです。

- **サーバタイプ(設定必須)(★)**

  Firewall用、管理サーバ用を選択してください。

- **ホスト名(設定必須)(★)**

  ホスト名はドメイン名まで含めたFQDN形式で入力してください。

- **インタフェースのIPアドレスとネットマスク、MTU値(設定必須)**

  Firewallでは、最低2つの設定が必要です。3つ目以降は任意です。管理サーバでは、最低1つの設定が必要です。途中のインタフェース(LANポート番号)を飛ばしての設定はできません。最大設定数は10個です。MTU値の設定範囲は、68～1500です。

- **ネームサーバのIPアドレス**

  最大3つのネームサーバを指定できます。入力を省略した場合、DNSによる名前解決は行いません。

- **管理者のメールアドレス(設定必須)(★)**

  1つのメールアドレスのみ設定できます。

- **メールゲートウェイのホスト名またはIPアドレス**

  システムがメールを送信する時にSMTP接続するメールサーバのIPアドレスを指定します。ホスト名で指定する場合はFQDN形式で入力してください。ただし、ネームサーバでその名前からIPアドレスが引ける必要があります。ネームサーバのIPアドレスを省略した場合、本項目は必ずIPアドレスを指定してください。

  本項目は省略可能ですが、その場合はFireWall-1や二重化機能などシステムが発信するメールはローカルのrootユーザー宛てに配送されます。本項目を省略した場合は定期的にメールをチェック、削除し、メールによってディスクを圧迫することがないように注意してください。また、FireWall-1や二重化機能では緊急時にメールで警告を通知することがあるため、本項目は必ず設定することをお勧めします。

- **デフォルトゲートウェイのIPアドレス(設定必須)(★)**

  1つのIPアドレスのみ設定できます。

- **(静的)ルーティングテーブル(★)**

  宛先アドレスとネットマスクおよびゲートウェイの組み合わせを指定します。
  本項目は省略することもできます。動的ルーティングはサポートしません。
  最大設定数は1000です。

- **Trap送信先IPアドレス**

  Trap送信先(ESMPRO/ServerManager)のIPアドレスを指定します。
  ESMPRO/ServerManagerとの連携を行わない場合は設定を省略することができます。
  最大設定数は1000です。

- **NTP (時刻同期)サーバのIPアドレス**

  NTP(時刻同期)サーバのIPアドレスを指定します。本項目は設定を省略することができます。最大設定数は1000です。

- **FireWall-1で取得されるログの保存日数(設定必須)**

  1〜90日の範囲で設定ができます。

- **二重化機能の設定**

  二重化構成を使用する場合に設定します。詳しくは4章を参照してください。

- **WbMCの設定(★)**

  WbMCを使用する場合に設定します。<Y>か<N>を入力します。

  また、WbMCを使用する場合は、ポート番号(1024〜65535)、管理クライアントのIPアドレス、管理者名(15文字以内)、httpsの使用/不使用を入力します。

- **SSHの設定(★)**

  SSHを使用する場合に設定します。<Y>か<N>を入力します。

  また、SSHを使用する場合は、ポート番号(1024〜65535)、管理クライアントのIPアドレス、管理者名(15文字以内)を入力します。

- **WbMCのパスワード設定(★)**

  WbMCを使用をする場合は、パスワードの入力、変更を行います。使用しない場合は、パスワード入力は行いません。

- **SSHのパスワード設定(★)**

  SSHを使用する場合は、パスワードの入力、変更を行います。使用しない場合は、パスワード入力は行いません。

- **rootユーザーのパスワード変更**

  省略できますが、セキュリティ上変更することをお勧めします。パスワードを変更する場合は、<Y>を入力した後、新しいパスワードを入力します。また、WbMC、SSHを使用しない場合は、rootのパスワードのみの設定になります。

- **現在の時刻設定**

  時刻を修正する場合は <Y> を入力した後、8桁もしくは12桁で現在の時刻を入力します。省略可能です。

- **サービスの起動と停止(設定必須)**

  起動時に必要なサービスを起動、および不要なサービスを停止させるための設定ができます。必ず最初の1度目は実行してください。

重要

上記の設定後は、Firewall本体を再起動させてください。

設定例

前述の「初期導入設定用ディスクによる設定」-「入力項目の設定」に示すネットワーク構成を例にして基本設定ツールの使い方を説明します。

```
# fwsetup ................................................ ①

Firewall Server configuration tool Ver.2.1

server type
  1. Firewall
  2. Management Server
select number[1]: 1 ..................................... ②

hostname[fws.nec.co.jp]: ................................ ③

No.  IF address      netmask          mtu ┐
  1  192.168.1.126   255.255.255.0   1500 │ ............ ④
  2  202.247.5.126   255.255.255.0   1500 ┘
("a"=add | "m num"=modify | "d num"=delete | "l"=list | Enter=next): a ..... ⑤
interface address(3): 172.16.1.126
netmask(3): 255.255.255.0
mtu(3)[1500]: 1500
interface address(4):
No.  IF address      netmask          mtu
  1  192.168.1.126   255.255.255.0    1500
  2  202.247.5.126   255.255.255.0    1500
  3  172.16.1.126    255.255.255.0    1500
("a"=add | "m num"=modify | "d num"=delete | "l"=list | Enter=next):
```

① 初期設定ツールを起動する。

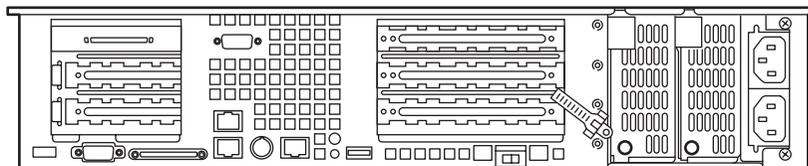
② Firewall/管理サーバを設定する。

Firewallとして設定するので、[1]を選択します。

③ ホスト名を設定する。

ホスト名はFQDN形式で入力してください。初期導入設定用ディスクにて設定済みの場合は、再度入力する必要はありません。入力済みになっていますので<Enter>キーを入力してください。

④ インタフェース別にIPアドレスとネットマスク、MTU値を設定する。

初期導入設定用ディスクで設定しているので、一覧が表示されます。

⑤ インタフェースの設定を追加する。

前述のネットワークインタフェースの設定で割り当てたインタフェースに対してのIPアドレスの設定を追加してください。
一覧から設定内容の追加、および修正、削除、一覧表の再表示をキー入力から操作できます。

<A>キー + <Enter>キー: ポートの設定を追加する。
<M>キー +「変更するポート番号」+ <Enter>キー: 指定したポートの設定を変更する。
<D>キー +「削除するポート番号」+ <Enter>キー: 指定したポートの設定を削除する。
<L>キー + <Enter>キー: リストを再表示する。
<Enter>キー: 次の項目へスキップする。

```
nameserver(1): 192.168.1.2                                          ①
nameserver(2):
No. nameserver address
1 192.168.1.2
("a"=add | "m num"=modify | "d num"=delete | "l"=list | Enter=next):

administrator e-mail address[xyz@nec.co.jp]:                        ②

use mail gateway? (y/n)[n]: y                                       ③
mail gateway: 192.168.1.2

default gateway IP address[202.247.5.254]:                          ④

static routing                                                      ⑤
destination(1): 192.168.2.0                                         ⑥
netmask(1): 255.255.255.0
gateway(1): 192.168.1.254
destination(2):
No. destination netmask gateway
1 192.168.2.0 255.255.255.0 192.168.1.254
 ("a"=add | "m num"=modify | "d num"=delete | "l"=list | Enter=next):
```

① ネームサーバのIPアドレスを設定する(任意)。

② 管理者のメールアドレスを設定する。

初期導入設定用ディスクで設定した値が表示されますので、設定内容を確認して〈Enter〉キーを押してください。

③ メールゲートウェイのIPアドレスを設定する。

<Y>キーを押して値を入力します。省略する場合は<N>キーを押してください。

④ デフォルトゲートウェイのIPアドレスを設定する。

初期導入設定用ディスクで設定した値が表示されますので、設定内容を確認して〈Enter〉キーを押してください。

⑤ ルーティングテーブルを設定する(任意)。

⑥ 宛先のIPアドレス(ネットワークアドレス)、ネットマスク、およびそのネットワークへのゲートウェイアドレスを設定する。

初期導入設定用ディスクで設定済みの場合は、設定した内容のリストが表示されます。

```
trap sink host(1): 192.168.1.10 ············ ①
trap sink host(2):
No. trap sink host
1 192.168.1.10
("a"=add | "m num"=modify | "d num"=delete | "l"=list | Enter=next):

NTP server address(1): 192.168.1.3 ············ ②
NTP server address(2):
No. NTP server address
1 192.168.1.3
("a"=add | "m num"=modify | "d num"=delete | "l"=list | Enter=next):

log file rotation(days) [30]: 30 ············ ③

Use cluster system? (y/n)[n]: n ············ ④

use firewall Web Management Console(WbMC) (y/n)[y]: y ············ ⑤
change firewall WbMC configuration? (y/n)[n]: y ············ ⑥
port( 1024 - 65535 )[18000]: 18000············ ⑦
No.  available host ip address
  1  192.168.1.99
("a"=add | "m num"=modify | "d num"=delete | "l"=list | Enter=next): ············ ⑧
use https? (y/n)[y]:y ············ ⑨
available user(with in 15 character)[fws-admin]:············ ⑩
```

① trap送信先IPアドレスを設定する（任意）。

ESMPRO/ServerManagerがインストールされているマシンのIPアドレスを設定してください。

② NTP（時刻同期）サーバのIPアドレスを設定する（任意）。

③ FireWall-1で取得されるログの保存日数を設定する。

④ 二重化機能に関する問い合わせメッセージ。

二重化機能を使用しない場合、<N>キーを押してください。

二重化機能を使用する場合で二重化のためのポリシー設定が、未設定の場合<N>キーをを、設定済みの場合は<Y>キーを押してください。詳しくは4章を参照してください。

⑤ WbMCの使用/未使用を設定をする。

<Y>キーか<N>キーを押します。

⑥ WbMCの設定を行う。

<Y>キーを押して、次へ進みます。初期導入設定用ディスクで設定した値が表示されますので、設定内容を確認して<Enter>キーを押してください。確認が不要な場合には、<N>キーを押してください。

⑦ ポート番号を入力する。

既定値は、18000です。

⑧ 使用者のホストのIPアドレスを入力する。

最大使用可能ホスト数は、100です。

⑨ httpsを使用する場合は、<Y>キーを押します。

⑩ 使用者の名前を登録する。
最大文字数は、15文字です。

```
use secure shell(SSH) (y/n)[y]: y ························ ①
change SSH configuration? (y/n)[n]: y ···················· ②
port( 1024 - 65535 )[18022]: ····························· ③
No.  available host ip address
  1  192.168.1.99
("a"=add | "m num"=modify | "d num"=delete | "l"=list | Enter=next): ···· ④
available user(with in 15 character)[fws-admin]: ········· ⑤

once again input? (y/n)[n]: n ···························· ⑥

[WbMC] change passward for user fws-admin? (y/n)[n]: n ··· ⑦

[SSH] change passward for user fws-admin? (y/n)[n]: n ···· ⑧
```

① SSHの使用/未使用を設定する。

<Y>キーを押します。

② SSHの設定の設定を行う。

<Y>キーを押して、次へ進みます。初期導入設定用ディスクで設定した値が表示されますので、設定内容を確認して<Enter>キーを押してください。確認が不要な場合には、<N>キーを押してください。

③ ポート番号を入力する。

default値は、18022です。

④ 使用者のホストのIPアドレスを入力する。

最大使用可能ホスト数は、100です。

⑤ 使用者の名前を登録する。

最大文字数は、15文字です。

⑥ ここまでの設定項目について設定を変更したいときは<Y>キーを押す。次に進む場合は、<N>キーを押す。

⑦ 運用監視ツールの使用者のパスワードを入力する。

パスワードは推測されにくいものを用意してください。
初期導入設定用ディスクで設定済の場合は、再入力の必要はありません。<N>を入力し次へ進みます。

⑧ SSHの使用者のパスワードを入力する。

パスワードは推測されにくいものを用意してください。
初期導入設定用ディスクで設定済の場合は、再入力の必要はありません。<N>を入力し次へ進みます。

```
change root password? (y/n)[n]: y ········· ①
Changing password for user root.
New UNIX password:
Retype new UNIX password:
passwd: all authentication tokens updated successfully

Fri Sep 6 16:48:44 JST 2002
set date and time? (y/n)[n]: y ········· ②
date and time (MMDDhhmm[[CC]YY]): 09061653
Fri Sep 6 16:53:01 JST 2002
set date and time? (y/n)[n]:

replace startup-scripts? (y/n)[n]: y ········· ③

Please reboot the system.

#shutdown -r now ········· ④
```

① 出荷時に設定されているパスワードを変更する。

セキュリティのためにも、出荷時のパスワードから変更することをお勧めします。
パスワードは推測されにくいものを用意してください。

② 時刻の設定を変更する。

③ 必要なサービスの起動および不要なサービスの停止を行う（必須）。

ここでは必ず<Y>キーを押してください。

④ 設定を有効にするため、システムを再起動する。

重要

fwsetupを実行した際、以下のようなメッセージが表示されることがあります。

```
# fwsetup
Firewall Server configuration tool Ver.2.1
fwsetup is under use...
#
```

この場合、他のユーザーがfwsetupを実行している可能性がありますので、他のユーザーの使用状況を確認した後、再度fwsetupを実行してください。
また、他のユーザーがfwsetupを実行していないことが確認された場合、以下のコマンドを実行した後、再度fwsetupを実行してください。

```
# rm -f /var/opt/necfws/lock/fwsetup
```

FireWall-1のコンフィグレーション

次に管理クライアントからFireWall-1付属のcpconfigコマンドを実行します。以下の手順でコンフィグレーションを行ってください。

```
# cpconfig ........................................................ ①
Welcome to Check Point Configuration Program
============================================
Please read the following license agreement. ...................... ②
Hit 'ENTER' to continue...

This End-user Lisences Agreement (the "Agreement") is an agreement
between you (both the individual installing the Product and any legal
entity on whose behalf such individual in acting) (hereinafter "You"
or "Your") and Check Point Software Technologies ltd. (hereinafter
"Check Point").
                              :
                              :
                              :
Do you accept all the terms of this license agreement? (y/n) ? y .... ③

Select installation type:
-------------------------
(1) Enforcement Module
(2) Enterprise Management
(3) Enterprise Management and Enforcement Module
(4) Enterprise Log Server
(5) Enforcement Module and Enterprise Log Server

Enter your selection (1-5/a) [1]: 3 .................................. ④
```

① FireWall-1のコンフィグレーションをする「cpconfig」コマンドを実行する。

② 〈Enter〉キーを押す。

使用許諾書が表示されますのでお読みください。

③ 使用許諾に承認した場合は〈Y〉キーを押す。

④ インストールするモジュールを選択する。

「3」を選択して、一体型構成でインストールします。

```
Please select Managemet type:
-----------------------------
(1) Enterprise Primary Management
(2) Enterprise Secondary Management

Enter your selection (1-2/a-abort) [1]: 1 ······························· ①

Would like to enable SecureXL acceleration feature? (y/n) [y] ? n ········ ②
IP forwarding disabled
Hardening OS security: IP forwarding will be disabled during boot.
Generating default filter
Default Filter installed
Hardening OS Security: default Filter will be applied during boot.
This prgram will guide you through several steps where you
will define your VPN-1 & Firewall-1 configuration.
At any later time, you can reconfigure these parameters by
running cpconfig

Configuring Licenses...
=======================
Host           Expiration Signature          Features

Note: The recommended way of managing licenses is using SecureUpdate.
This window can be used to manage local licenses only on this machines.

Do you want to add licenses (y/n) [n] ? y ······························· ③

Do you want to add licenses [M]anually or [F]etch from file: m ·········· ④
IP Address:202.247.5.126 ┐
Expiration Date:         │
Signature Key:           ├──────────────────────────────────────────────── ⑤
SKU/Features:            ┘

License was added successfully

License will be put into kernel after cpstart
```

① インストールするFireWall-1のタイプを選択する。

通常は「1」を選択し、Primaryとして使用します。

② SecureXLの使用/未使用を設定する。

本製品では、SecureXLを使用しません。〈N〉を選択します。

③ 〈Y〉キーを押して、ライセンスを追加する。

④ 〈M〉キーを押して、ライセンスを画面から(マニュアルで)登録する。

⑤ 事前に取得したライセンス情報を入力する。

ライセンスは、Firewallのライセンス製品に同梱されている「ライセンス申請書」をNSSolへFAXし、取得してください。本製品(Express5800/FW500)には「ライセンス申請書」は含まれていません(1章の「Express5800/FW500の製品体系」を参照してください)。

```
Configuring Administrators...
=============================
No VPN-1 & FireWall-1 Administrators are currently
defined for this Management Station.

Do you want to add administrators (y/n) [y] ? y ............ ①

Administrator name: fws-admin
Password:
Verify Password:                                ............ ②
Permissions for all Management Clients (Read/[W]rite All, [R]read Only All,
[C]ustomized) w ............................................ ③

               Permission to Manage Administrators ([Y]es, [N]o) y ...... ④

Administrator fws-admin was added successfully and has
Read/Write Permission for all Management Clients

Add another one (y/n) [n] ? n .............................. ⑤
```

① <Y>キーを押して、管理者を追加する。

② Firewall (FireWall-1)の管理者名、およびパスワードを設定する。

③ 書込み/読込みが可能となるように<W>を選択する。

④ 管理者の権限を設定する。

作成した管理者にManageの権限を付与します。

⑤ 管理者を追加する場合は<Y>キーを、登録を終了する場合は<N>キーを押す。

```
Configuring Mangement Clients...
================================
Management Clinet are trusted hosts from which
Administrators are allowed to log on to this Mnanagement Station
using Windows/X-Motif GUI.

No Management Client defined

Do you want to add a Management Client (y/n) [y] ? y ......... ①
Please enter the list hosts that will be Management Clients.
Enter hostname or IP address, our per line, terminating with CTRL-D or your EOF
character.
192.168.1.99 ......... ②
Is this correct (y/n) [y] ? y ......... ③


Configuring Random Pool...
==========================
You are now asked to perform a short random keystroke session.
The random data collected in this session will be used in
various cryptographic operations.

Please enter random text containing at least six different
characters. You will see the '*' symbol after keystrokes that
are too fast or too similar to preceding keystrokes. These
keystrokes will be ignored.

Please keep typing until you hear the beep and the bar is full.

    [....................] ......... ④

Thank you.
```

① <Y>キーを押して、管理クライアントのIPアドレスリストを作成する。

② セキュリティポリシーの設定を行う管理クライアントのIPアドレスを設定する。

複数のIPアドレスを設定する場合は改行して複数行入力します。入力を終了する場合は<Ctrl>-<D>キーを押します。

③ 入力したアドレスが正しければ<Y>キーを押す。

④ バーがフルになるまでランダムキーを入力する。

```
Configuring Certificate Authority...
=====================================
The system uses an internal Certificate Authority
to provide Secured Internal Communication (SIC) Certificateies
for the components in your System.

Note that your components won't be able to communicate
with each other until the Certificate Authority is initialized
and they have their SIC certificate.

Press 'Enter' to initialize the certificate Authority... ……… ①
 Internal Certificate Authority created successfully
 Certificate was created successfully
Certificate Authority initialization ended successfully


The FQDN (Fully Qualified Domain Name) of this Management Server
is required for proper operation of the International Certificate Authority.

Would you like to define it now (y/n) [y] ? y ……… ②
The FQDN of this Management Server is fws.nec.co.jp
Do you want to change it (y/n) [n] ? n ……… ③


NOTE: If the FQDN is incorrect, the Internal CA cannot function properly,
and CRL retrieval will be impossible.

Are you sure fws.nec.co.jp is the FQDN of this machine (y/n) [n] ? y ……… ④

Press 'Enter' to send it to the Certificate Authority....

Trying to contact CA. It can take up to 4 seconds...
 FQDN initialized successfully

The FQDN was successfully sent to the CA
```

① インターナルCA(Certificate Authority)の設定を行う。

<Enter>キーを押してください。

② FQDNの設定を行う。

<Y>を選択します。

③ 変更の必要はないので、そのまま<N>を選択する。

④ 表示されているFQDNを確認し<Y>キーを押す。

```
Configuring Certificate's Fingerprint...
========================================
The following text is the fingerprint of this Management machine:
XXXX XXXX XXXX XXXX XXXX XXXX XXXX XXXX XXXX XXXX XXXX XXXX


Do you want to save it to a file? (y/n) [y] ? n ……………………… ①
generating GUI-clients INSPECT code
initial_management:
Compiled OK.

Hardening OS Security: Initial policy will be applied
until the first policy is installed

In order to complete the installation
you must reboot the machine.
Do you want to reboot? (y/n) [y] ? y ……………………… ②
```

① GUIクライアントを接続したとき、接続したFireWall-1が正しいものであるかどうかを確認するため文字列が表示されるので、この文字列をディスク上に保存する場合は<Y>キーを、保存しない場合は、<N>キーを押す。

② 終了後、再起動する。

再起動後は、FireWall-1のデフォルトフィルタが有効になるため、SSH、WbMCでの接続が不可となります。

3. セキュリティポリシーのセットアップ

セキュリティ機能をセットアップする「SmartDashboard」を管理クライアントにインストールし、編集したポリシーをインストールします。
次の条件を満たすコンピュータにSmartDashboardやその他のツールをインストールして、クライアントマシンとして使用します。

- オペレーティングシステム: Windows XP Home/professional、
  Windows 98/Me、
  Windows NT 4.0 Workstation(SP6a)、
  Windows NT 4.0 Server(SP6a)、
  Windows 2000 Professional(SP1、SP2、SP3)、
  Windows 2000 Server(SP1、SP2、SP3)、
  Windows 2000 Advanced Server(SP1、SP2)
- ディスク空き容量: 55MB以上
- メモリ: 128MB以上

* 上記は2002年11月現在の情報です。今後のパッチリリースにより変更になる可能性があります。

重要 **GUIクライアントのインストールにおいて、画面イメージが、FeaturePackによって異なる場合があります。**

GUIクライアントのインストール

管理クライアントにSmartDashboardをインストールします。ここでは、SmartDashboardといっしょにログを解析するためのツール「SmartView Tracker」とシステムの状態をチェックする「SmartView Status」もインストールします。

1. コンピュータのCD-ROMドライブにCheck Point Next GenerationのCD-ROMをセットする。

   自動的にインストールプログラムが起動し、画面が表示されます。
   インストールプログラムが起動しない場合は¥wrappers¥windowsフォルダにある「demo32.exe」を実行してください。

   Welcome画面が表示されます。

2. [Next]をクリックする。

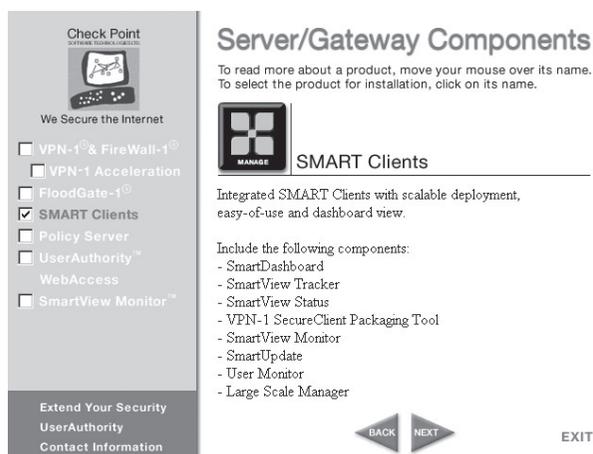
   使用許諾契約書が表示されます。

3. 内容をよく読み、同意する場合は[Yes]をクリックする。

   同意しない場合は[No]をクリックして終了します。
   プロダクトメニューの画面が表示されます。

4. ［SERVER/GATEWAY COMPONENTS］を選択し、［Next］をクリックする。

Componentsの選択画面が表示されます。

5. ［SMART Clients］のみをチェックして ［Next］をクリックする。

その他のコンポーネントのチェックは外します。

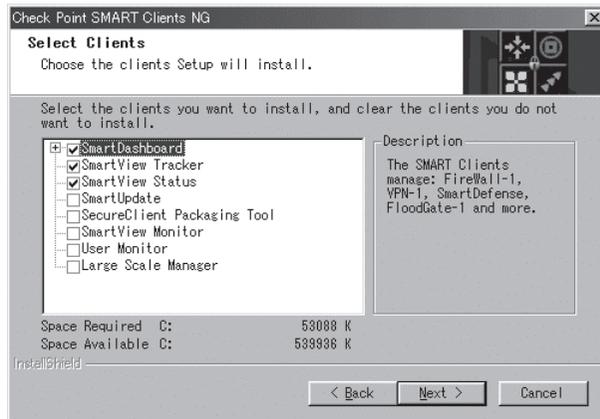
Check Point Installation program画面が表示されます。

6. 「SMART Client」と表示されていることを確認し、［Next］をクリックする。

インストール先のフォルダを指定する画面が表示されます。

7. 必要に応じてフォルダを変更し、［Next］をクリックする。

インストールするコンポーネントを選択する画面が表示されます。

8. [SmartDashboard]と[SmartView Tracker]、[SmartView Status]をチェックし、[Next]をクリックする。

その他のコンポーネントのチェックは外します。

インストールが開始されます。

9. インストール完了メッセージが表示されたら[OK]をクリックして終了する。

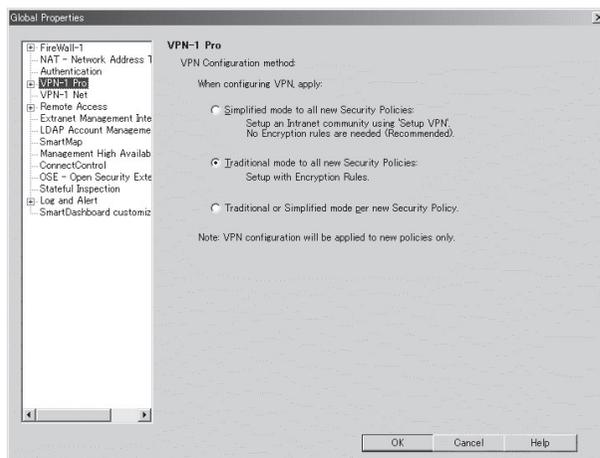
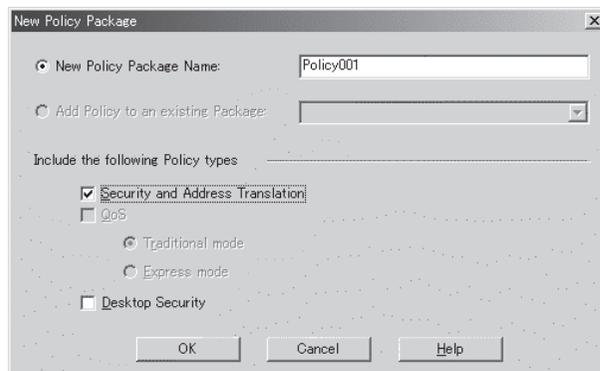
次にSmartDashboardを起動して、ポリシー画面の設定を行います。

10. SmartDashboardを起動し、cpconfig で登録したユーザ名とパスワード、およびFirewallの内側(管理クライアント側)のアドレスを入力する。

SmartDashboardを使用し、Firewallと接続してポリシーを作成します。ネットワーク構成に応じたポリシールールを作成してください。
SmartDashboardの使い方、セキュリティポリシーの設定等についてはFireWall-1に付属のマニュアルを参照してください。

ポリシーを作成する時は、以下の手順を用いてTraditional modeで作成することを推奨します。

11. Traditional mode の設定

SmartDashboardを起動し、接続されたらメニューバーから[Policy] - [Global Properties] のVPN-1 Proページにおいて、「Traditional mode to all new Security Policies: Setup with Encryption Rules.」を選択し、[OK]をクリックする。

12. メニューバーから [File] - [New] を選択し、Policy Package Nameを設定する。

13. 「Security and Address Translation」を選択して[OK]をクリックする。

新しいポリシー設定画面が作成され、ポリシーの設定が可能となります。

重要

Firewallと管理クライアントとの設定において、SSHを使用しますので、FireWall-1のポリシーに、管理クライアントからFirewallに対してSSHのポート番号へのアクセスを許可するためのルールを追加してください。このとき、接続元には必ず管理クライアントのみを設定し、他のホストからのアクセスは許可しないようにしてください。

【参考 1】WbMCを使用した設定手順の流れ

以下に、WbMCを使用したセットアップの概要を説明します。

WbMCの接続は、必ず内部ネットワークの管理クライアントから行ってください。外部から接続を許可する設定には絶対にしないでください。また、WbMCを使用する場合は、Internet Explorerバージョン5以上でご利用ください。

1. 初期導入設定用ディスクによる初期設定をする。

   初期導入設定用ディスクの設定については、前述の「初期導入設定用ディスクによる設定」を参照してください。

   チェック

   リモートメンテナンス機能の利用に関する設定において、「WbMCを使用する」にチェックをつけます。

2. 管理クライアントのWebブラウザを使用してFirewallのWbMCに接続する。

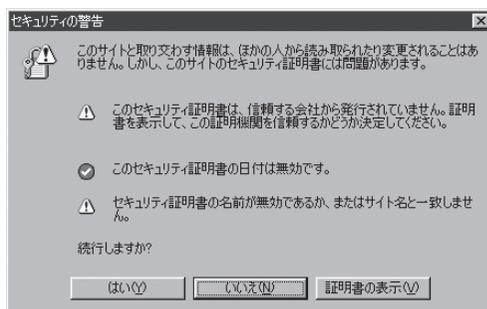
   このときのURLは、Firewallの内側(管理クライアントが設置されているネットワーク側)のインタフェースのIPアドレスを、ポート番号には初期設定、あるいは基本設定ツールで指定したポート番号を指定します。

   例) `https://192.168.1.126:18000/`

   192.168.1.126：Firewallの内側のインタフェースのIPアドレス
   18000：基本設定ツールで指定したポート番号

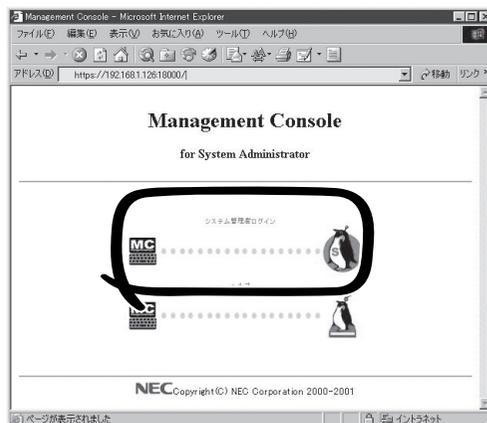
3. 接続すると、セキュリティの警告が表示される。

   [はい]をクリックします。

4. ユーザー名とパスワードの問い合わせがありますので、初期設定、あるいは基本設定ツールで設定した管理者名とパスワードを入力する。

   接続に成功すると、右の画面が表示されます。

5. 四角で囲まれた部分をクリックする。

   左側にメインメニューを表示する「Menu領域」、右側に「メイン領域」が表示されます。

6. 左側のメニューから「基本設定」を選択して設定を行ってください。

   重要

   FireWall-1のポリシーに、管理クライアントからFirewallに対してWbMCのポート番号へのアクセスを許可するためのルールを追加します。このとき、接続元には必ず管理クライアントのみを設定し、他のホストからのアクセスは許可しないようにしてください。

【参考 2】コンソールを使用した設定手順の流れ

本体の電源がOFFの状態で、管理クライアントを本体背面にあるシリアルポート2(COM2)に接続し、システムを起動してください。

- **本体に接続するために必要なもの**

  ー シリアルインタフェース(RS232C)を持ったコンピュータ

  ー 通信用ソフトウェア(例：Windows 2000 ハイパーターミナル)

  ー シリアルケーブル(クロス)

  ー RJ45と9pin変換コネクタ(K410-110(00))

  K210-84(05)(9pin-9pin)またはK208-12(03)(9pin-25pin)のうち、お手持ちのコンピュータに適合するケーブルをご利用ください。

- **ケーブルの接続**

  本体背面にあるシリアルポート2(COM2)にシリアルケーブル(クロス)を接続してください。

- **ターミナルエミュレータの設定**

  ターミナルエミュレータのパラメータは以下のように設定してください。

  ボーレート　　：19,200bps

  パリティ　　　：なし

  キャラクタ長　：8bit

  ストップビット：1bit

- **管理クライアントの接続**

  本体の電源を投入後、しばらく(3分程度)してから管理クライアントの<Enter>キーを押すと、管理クライアントのディスプレイにloginプロンプトが表示されます。

  管理クライアントから「root」と入力し、「Password」に同梱の「rootパスワード」に書かれているパスワードを入力します。ログインに成功すると「#」のプロンプトが表示されます。

  重要 **rootのパスワードは、基本設定ツールで出荷時のパスワードから変更してください。**

以下に、コンソールを使用したセットアップの手順概要を説明します。

1. Firewall本体にコンソールを接続してログインする。

2. 基本設定ツール(fwsetup)を実行して設定をする。

   設定については、本章の「2. システムのセットアップ」を参照してください。

3. FireWall-1のコンフィグレーション(cpconfig)の設定をする。

   コンフィグレーションの設定については、本章の「2. システムのセットアップ」-「FireWall-1のコンフィグレーション」を参照してください。

4. セキュリティポリシーのセットアップとインストールをする。

   本章の「3. セキュリティポリシーのセットアップ」を参照してください。

4. バックアップ

万一の故障による再インストールに備えて、設定したセキュリティポリシーのバックアップを作成します。バックアップの取得方法は2種類あります。

重要

バックアップを取得する際には、Firewallの運用を一時的に中断させなければいけません。

コマンドによるバックアップ取得

fwbackupコマンドを管理クライアントから実行するとフロッピーディスクのセットを要求するメッセージが表示されます。
フロッピーディスクをセットして<Enter>キーを押すと、後は自動的にフロッピーディスクへバックアップします。
バックアップコマンド実行時、バックアップに必要なフロッピーディスクの枚数が表示されるので、必要数のフロッピーディスクをあらかじめ用意してください。

通常はフロッピーディスク1枚でバックアップ可能ですが、ポリシーのルール数やユーザー登録数が極端に多い場合などは1枚に保存できないことがあります。ファイルがフロッピーディスク1枚に保存できない場合には、複数枚のフロッピーディスクに分割してバックアップコピーを行います。メッセージに従ってフロッピーディスクを入れ換えてください。

重要

バックアップディスクには、必ずDOSフォーマット(1.44MB)済みのブランクディスクを使用してください。

```
# cpstop
# fwbackup
1 floppy disk is needed for backup.
Please insert DOS formatted(1.44MB) floppy disk(#1).
Press enter key.
backup fws.ini...
backup .http...
backup .ssh...
backup clp.conf...
back up fw config files...
back up fws registory files...
back up completed.
After turned off FDD access light, Press enter key.
# cpstart
```

5. ESMPRO/ServerAgentのセットアップ

ESMPRO/ServerAgentは出荷時にインストール済みですが、固有の設定がされていません。以下のオンラインドキュメントを参照し、セットアップをしてください。

添付のバックアップCD-ROM:/nec/Linux/esmpro/doc/users.pdf

ESMPRO/ServerAgentの他にも「エクスプレス通報サービス」(5章参照)がインストール済みです。ご利用には別途契約が必要となります。詳しくはお買い求めの販売店または保守サービス会社にお問い合わせください。

シリアル接続の管理クライアントから設定作業をする場合は、管理者としてログインした後、設定作業を開始する前に環境変数「LANG」を「C」に変更してください。デフォルトのシェル環境の場合は以下のコマンドを実行することで変更できます。

```
#export LANG=C
```


6. システム情報のバックアップ

システムのセットアップが終了した後、添付の「保守・管理ツールCD-ROM」にあるオフライン保守ユーティリティを使って、システム情報をバックアップすることをお勧めします。システム情報のバックアップがないと、修理後にお客様の装置固有の情報や設定を復旧(リストア)できなくなります。次の手順に従ってバックアップをしてください。

保守・管理ツールCD-ROMからシステムを起動して操作します。保守・管理ツールCD-ROMから起動させるためには、事前にセットアップが必要です。5章の「保守・管理ツール」を参照して準備してください。

1. 3.5インチフロッピーディスクを用意する。
2. 装置に添付の「保守・管理ツールCD-ROM」から「オフライン保守ユーティリティ」を起動する。

   「保守・管理ツールCD-ROM」の使い方については5章の「保守・管理ツール」を参照してください。
3. [システム情報の管理]から[退避]を選択する。

   以降は画面に表示されるメッセージに従って処理を進めてください。

7. 管理コンピュータのセットアップ

本装置をネットワーク上のコンピュータから管理・監視するためのアプリケーションとして、「ESMPRO/ServerManager」と「Management Workstation Application(MWA)」が用意されています。
これらのアプリケーションを管理コンピュータにインストールすることによりシステムの管理が容易になるだけでなく、システム全体の信頼性を向上することができます。

ESMPRO/ServerManagerとMWAのインストールについては5章、または保守・管理ツールCD-ROM内のオンラインドキュメントを参照してください。

再セットアップ

再セットアップとは、システムの破損などが原因でシステムが起動できなくなった場合などに、添付の「バックアップCD-ROM」を使ってハードディスクを出荷時の状態に戻してシステムを起動できるようにするものです。以下の手順で再セットアップをしてください。

保守用パーティションの作成

「保守用パーティション」とは、装置の維持・管理を行うためのユーティリティを格納するためのパーティションで、16MB程度の領域を内蔵ハードディスク上へ確保します。
Firewallの信頼性を向上するためにも保守用パーティションを作成することをお勧めします。
保守用パーティションは、添付の「保守・管理ツールCD-ROM」を使って作成します。詳しくは5章の「保守・管理ツール」を参照してください。

保守用パーティションを作成するプロセスで保守用パーティションへ自動的にインストールされるユーティリティは、「システム診断ユーティリティ」と「オフライン保守ユーティリティ」です。

システムの再インストール

ここでは、システムの再インストールの手順について説明します。
二重化構成を構築している場合は、再インストールの手順が異なります。4章の「二重化構成の再セットアップ」を参照してください。

再インストールを行うと、装置内の全データが消去され、出荷時の状態に戻ります。必要なデータが装置内に残っている場合、データをバックアップしてから再インストールを実行してください。

再インストールの準備(SSH接続)

作業を行うためには、SSH接続用管理クライアントが必要です。本体の電源がOFFの状態で、SSH接続用管理クライアントを本体背面のLANポートインタフェース(内部ネットワーク用)にクロスケーブル接続してください。また、Firewallに直接LANケーブルを接続しないで、内部ネットワークに接続する場合は、ハブなどにLANケーブルで接続してください。

Firewallとの接続に必要なもの

- SSH接続用管理クライアント
- LANケーブル

再インストールに必要なディスク

あらかじめ以下のディスクを用意してください。

- バックアップCD-ROM
- Check Point Next Generation (Feature Pack3)
- 再インストール用ディスク
- 初期導入設定用ディスク
- バックアップディスク(任意)

再インストールの手順

1. 本体の電源を入れ、前面にあるフロッピーディスクドライブに再インストール用ディスクを、CD-ROMドライブにバックアップCD-ROMをセットする。

2. 自動的にプログラムCD-ROMからのインストールが始まる。

   インストールは約10分で完了します。
   インストールを完了すると、CD-ROMドライブからバックアップCD-ROMが排出されます。
   本体は、電源が入った状態で、システムが停止している状態になります。

3. バックアップCD-ROMおよび再インストール用ディスクを取り出した後、POWERスイッチを押して電源を切る。

4. 初期導入設定用ディスクをセットし、POWERスイッチを押して電源を入れる。

   初期導入設定用ディスクは、初期導入設定用ツールで作成済みのものとします。
   しばらく(3分程度)してから管理クライアントからSSHクライアントにて、Firewallへログインします。

5. 管理クライアントから初期導入設定用ディスクで設定したSSHの「管理者アカウント名」と「Password」を利用し、ログインする。

6. <バックアップしておいた設定をリストアする場合>

   以下のコマンドを実行して設定を行う。

   設定をバックアップしたフロッピーディスクを本体にセットしてください。

   <バックアップのリストアをしない場合>

   本章の「2. システムのセットアップ」-「基本設定ツールによる設定」を参照して設定を行う。

7. 終了後、再起動する。

8. 起動後、CD-ROMドライブにCheck Point Next Generation(Feature Pack3)のCD-ROMをセットし、FireWall-1のモジュールを以下の手順で適用する。

```
# mount /dev/cdrom
# cd /mnt/cdrom/linux/

# rpm -i ./CPshared-50/CPshrd-50-03.i386.rpm
# rpm -i ./CPFirewall1-50/CPfw1-50-03.i386.rpm

# cd /
# umount /dev/cdrom
```

9. CD-ROMドライブからCD-ROMを取り出し、再起動する。

```
# shutdown -r now
```

10. cpconfigを実行してFireWall-1の設定を行う。

cpconfigについては本章の「2. システムのセットアップ」-「FireWall-1のコンフィグレーション」を参照してください。

```
# cpconfig
     :
     :
Do you wish to start the installed product(S) now? (y/n) [y] ? y
```

11. ポリシーの作成を行う。

<あらかじめバックアップしておいた設定をリストアする場合>
以下のコマンドを実行してFireWall-1の設定をする。

```
# cpstop                      ―― FireWall-1を停止する
# fwrestore -f

Please insert backup floppy disk. (#1)
Press enter key.              ―― バックアップディスクをセットして、<Enter>キーを押す
There is 1 floppy disk for restore.
restore fw config files...(1/1)
restore completed.
After turned off FDD access light, Press enter key.
# cpstart
```

FireWall-1を起動する（cpstart）

フロッピーディスクドライブのアクセスランプが消えたら<Enter>キーを押し、その後フロッピーディスクを取り出す（After turned off FDD access light, Press enter key.）

<バックアップのリストアをしない場合>

SmartDashboardを使用してポリシーを作成する。

12. SmartDashboardでポリシーをインストールする。

重要

CD-ROMドライブにCheck Point Next Generation(Feature Pack3)のCD-ROMをセットした状態のままFirewall本体を起動しないように注意してください。

ESMPRO/ServerAgentのセットアップ

「システムの再インストール」でESMPRO/ServerAgentは自動的にインストールされますが、固有の設定がされていません。以下のオンラインドキュメントを参照し、セットアップをしてください。

添付のバックアップCD-ROM:/nec/Linux/esmpro/doc/users.pdf

ESMPRO/ServerAgentの他にも「エクスプレス通報サービス」(5章参照)も自動的にインストールされます。

シリアル接続の管理クライアントから設定作業をする場合は、管理者としてログインした後、設定作業を開始する前に環境変数「LANG」を「C」に変更してください。デフォルトのシェル環境の場合は以下のコマンドを実行することで変更できます。

```
#export LANG=C
```

システム情報のバックアップ

システムの再セットアップが終了した後、添付の「保守・管理ツールCD-ROM」にあるオフライン保守ユーティリティを使って、システム情報をバックアップすることをお勧めします。前述の「システム情報のバックアップ」、および5章の「保守・管理ツール」を参照してください。